# UNITED STATES PATENT AND TRADEMARK OFFICE

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/625,817 | 07/26/2000 | Daniel Bleichenbacher | BLEICHENBACHER4-27 | 8285 |

| | | | EXAMINER |
|---|---|---|---|
| 27964 | 7590 | 11/03/2003 | KIANERSI, MITRA |

HITT GAINES P.C.
P.O. BOX 832570
RICHARDSON, TX  75083

| ART UNIT | PAPER NUMBER |
|---|---|
| 2143 | 4 |

DATE MAILED: 11/03/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

| Office Action Summary | Application No. | Applicant(s) |
|---|---|---|
| | 09/625,817 | BLEICHENBACHER ET AL. |
| | Examiner | Art Unit |
| | mitra kianersi | 2143 |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>03</u> MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on <u>26 July 2000</u>.

2a)☐ This action is **FINAL**.      2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) <u>1-21</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-21</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>July 26 2000</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

    If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

**Priority under 35 U.S.C. §§ 119 and 120**

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

        1.☐ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____.

        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

    a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) <u>2</u>.

4) ☐ Interview Summary (PTO-413) Paper No(s). _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: .

Claims 1-21 have been examined.

## *Specification*

On page 18 line 19 of specification, the application interface "243" appears

incorrect. It appears the correct number is "324". Correction is required.

## *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for

all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-21 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Juels et al. (Client Puzzles: a Cryptographic countermeasure against

connection depletion attacks: Proceedings of NDSS'99 (Network and distributed

security systems) and further in view of Shkedy (US Patent No. 6,236,972).

1.      Regarding claims 1, Juels et al. discloses a system for controlling access

to a resource of a computer system, comprising:

        - a problem retriever (corresponds to a server which distributes small

cryptographic puzzles to a client making service requests, abstract, lines 14-16)

that responds to a request from a client for access to resource by retrieving one

of problems and transmitting one of problems to client; (the server hands out to

each client wishing to make a connection a unique client puzzle, Pg 151, Col 2, Prg 2), and

- a solution evaluator that, upon receiving a putative solution from client, to validate putative solution and, if putative solution is valid, grants client access to resource.(the client must submit to the server a correct solution to the puzzle it have been given,(when the client sends its purported solution, the server can check if the entire puzzle is correctly solved. (Pg 156, Col 2, Prg 5).

Juels et al fail to teach employing a database to validate said putative solution.

However, Shkedy discloses a cryptographic database (element 290) for facilitating Cryptographic functions (col 10, lines 37-38) by incorporating a central controller database for matching sell and buy orders (corresponds to validating putative solutions) and executing a trade upon match (corresponds to granting client access to resource).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ a central controller database by Shkedy with Juels et al. system for controlling access to a resource in order to provide greater confidence in the authenticity of clients, because cryptographic protocols not only enhance the ability to authenticate the sender of message but also serve to verify the integrity of the message itself.


2.     Regarding claims 2, Juels-Shkedy discloses the invention substantially as discussed in claim 1 including system where problems comprise outputs and portions of corresponding inputs to a one-way function. (Shkedy, Col 18, lines 39-40)


3.     Regarding claims 3, Juels-Shkedy discloses the invention substantially as discussed in claim 2 including a system where one-way function is a Message Digest-5 function. (Shkedy, Col 18, lines 40-43)

4.      Regarding claims 4, Juels-Shkedy discloses the invention substantially as discussed in claim 1 including a system wherein problem retriever replaces one of said problems and a corresponding one of solutions when putative solution is valid. (Juels et al. Pg 152, Col 2, Prg 3, lines 3-9, corresponds to "syncookie approach")

5.      Claims 5, recites similar limitation as claim 4. The same rationale rejects it.

6.      Regarding claims 6, Juels-Shkedy discloses the invention substantially as discussed in claim 1, wherein solution evaluator grants client access to resource by allocating memory associated with said resource to serve client. (Juels et al. Pg 152, Col 1, Prg 3, lines 18-20. server allocates buffer space for each incomplete)

7.      Regarding claim 7, Juels-Shkedy disclose the invention substantially as discussed in claim 1, where a resource is selected from the group consisting of: network server (page 151, col 2, prg 2, line 12), and an electronic mail server (page 151, par 1, line 6), a main database (Shkedy col 10, lines 37-38, corresponds to a cryptographic database 290)

8.      Regarding claims 8-14, recites methods comprising similar limitations as to claim 1-7, respectively. Therefore, they are rejected by the same rationale set forth.

9.      Regarding claims 15, in addition to the rejection set forth in claim 1, Juels-Shkedy disclose employing a database of problems and corresponding precalculated solutions; (Shkedy, Page 1044-56, corresponds to a pointer that points to a particular problem/solution entry in said database.)

10.     Claim 16-21, recites similar limitations as claim 2-7. They are analyzed and rejected by the same rationale.

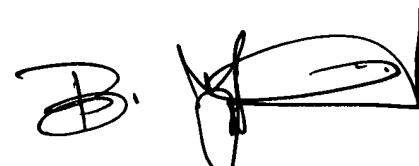## *Conclusion*

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mitra Kianersi whose telephone number is (703) 305-4650. The examiner can normally be reached on 7:00AM-4:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David Wiley can be reached on (703) 308-5221. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Mitra Kianersi
Oct/21/2003

BUNJOB JAROENCHONWANIT
PRIMARY EXAMINER